

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION
(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents
 United States Patent and Trademark
 Office
 Box PCT
 Washington, D.C.20231
 ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 23 August 1999 (23.08.99)	Applicant's or agent's file reference WWE-67196
International application No. PCT/US98/25824	Priority date (day/month/year) 05 December 1997 (05.12.97)
International filing date (day/month/year) 04 December 1998 (04.12.98)	
Applicant KOC, Cetin, Kaya et al	

1. The designated Office is hereby notified of its election made:

 in the demand filed with the International Preliminary Examining Authority on:

25 June 1999 (25.06.99)

 in a notice effecting later election filed with the International Bureau on:2. The election was was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer F. Baechler Telephone No.: (41-22) 338.83.38
---	---



European Patent
Office

**SUPPLEMENTARY
PARTIAL EUROPEAN SEARCH REPORT**

Application Number

which under Rule 45 of the European Patent Convention EP 98 96 5973
shall be considered, for the purposes of subsequent
proceedings, as the European search report

DOCUMENTS CONSIDERED TO BE RELEVANT			CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	
E	WO 99 43124 A (GEORGIADES JEAN ;HESS ERWIN (DE); SIEMENS AG (DE)) 26 August 1999 (1999-08-26) * page 7, line 1 - line 26; claims * ---	1,21-23	H04L9/30
X	KOC C K ET AL: "FAST SOFTWARE EXPONENTIATION IN GF(2 ^K)" PROCEEDINGS 13TH IEEE SYMPOSIUM ON COMPUTER ARITHMETIC. ASILOMAR, CA, JULY 6 - 9, 1997, IEEE SYMPOSIUM ON COMPUTER ARITHMETIC, LOS ALAMITOS, CA: IEEE COMP. SOC. PRESS, US, 6 July 1997 (1997-07-06), pages 225-231, XP000788129 ISBN: 0-8186-7846-1 * the whole document *	18-20	
A	-----	3-5,7-17	
TECHNICAL FIELDS SEARCHED (Int.Cl.6)			
G06F			
The supplementary search report has been based on the last set of claims valid and available at the start of the search.			
INCOMPLETE SEARCH			
The Search Division considers that the present application, or some or all of its claims, does/do not comply with the EPC to such an extent that a meaningful search into the state of the art cannot be carried out, or can only be carried out partially, for the following claims:			
Claims searched completely :			
Claims searched incompletely :			
Claims not searched :			
Reason for the limitation of the search:			
see sheet C			
1	Place of search	Date of completion of the search	Examiner
	THE HAGUE	12 December 2001	Verhoof, P
CATEGORY OF CITED DOCUMENTS		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document			

ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.

EP 98 96 5973

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

12-12-2001

Patent document cited in search report	Publication date		Patent family member(s)	Publication date
WO 9943124	A	26-08-1999	BR 9908095 A	31-10-2000
			CN 1297635 T	30-05-2001
			WO 9943124 A1	26-08-1999
			EP 1062764 A1	27-12-2000



European Patent
Office

INCOMPLETE SEARCH
SHEET C

Application Number
EP 98 96 5973

Claim(s) searched completely:
1-17,21-23

Claim(s) searched incompletely:
18-20

Reason for the limitation of the search (non-patentable invention(s)):

Claims 18-20 relate to a mathematical method, which is not patentable, according to Art. 52(2)(a). It is not clear how these claims could be modified to overcome this. The search for these claims was therefore limited to the mere use of Montgomery or the like arithmetic for finite field calculations.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To: SUZANNE J. HEEG
SHEPPARD MULLIN RICHTER & HAMPTON LLP
333 SOUTH HOPE STREET
48TH FLOOR
LOS ANGELES, CA 90071

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT OR THE DECLARATION

(PCT Rule 44.1)

Date of Mailing
(day/month/year)

12 APR 1999

Applicant's or agent's file reference
WWE-67196

FOR FURTHER ACTION See paragraphs 1 and 4 below

International application No.
PCT/US98/25824

International filing date
(day/month/year)

04 DECEMBER 1998

Applicant
SECURED INFORMATION TECHNOLOGY, INC.

1. The applicant is hereby notified that the international search report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19:

The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally 2 months from the date of transmittal of the international search report; however, for more details, see the notes on the accompanying sheet.

Where? Directly to the International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

2. The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. With regard to the protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Further action(s):** The applicant is reminded of the following:

Shortly after 18 months from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in rules 90 bis 1 and 90 bis 3, respectively, before the completion of the technical preparations for international publication.

Within 19 months from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within 20 months from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 19 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

RECEIVED

APR 16 1999

Authorized officer

DOUGLAS MEISLAHN

Telephone No. (703) 305-1338

Joni Hill

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference WWE-67196	FOR FURTHER ACTION	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
International application No. PCT/US98/25824	International filing date (day/month/year) 04 DECEMBER 1998	(Earliest) Priority Date (day/month/year) 05 DECEMBER 1997
Applicant SECURED INFORMATION TECHNOLOGY, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 5 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. Certain claims were found unsearchable (See Box I).
2. Unity of invention is lacking (See Box II).
3. The international application contains disclosure of a nucleotide and/or amino acid sequence listing and the international search was carried out on the basis of the sequence listing
 - filed with the international application.
 - furnished by the applicant separately from the international application,
 - but not accompanied by a statement to the effect that it did not include matter going beyond the disclosure in the international application as filed.
 - transcribed by this Authority.
4. With regard to the title, the text is approved as submitted by the applicant.
 the text has been established by this Authority to read as follows:
5. With regard to the abstract,
 - the text is approved as submitted by the applicant.
 - the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.
6. The figure of the drawings to be published with the abstract is:

Figure No. _____

 - as suggested by the applicant.
 - because the applicant failed to suggest a figure.
 - because this figure better characterizes the invention.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US98/25824

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.: 1-23
because they relate to subject matter not required to be searched by this Authority, namely:

The claims are to a mathematical theory. However, in accordance with the office's policy, a search has been done according to US standards.
2. Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

The additional search fees were accompanied by the applicant's protest.

No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/25824

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/30
US CL :380/28, 30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/28, 30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,E	US 5,854,759 A (KALISKI, JR. ET AL.) 29 December 1998, abstract	1-23
A,P	US 5,805,703 A (CRANDALL) 08 September 1998, abstract	1-23
A,P	US 5,751,808 A (ANSHEL ET AL.) 12 May 1998, abstract	1-23
A	US 5,581,616 A (CRANDALL) 03 December 1996, abstract	1-23
A	US 5,577,124 A (ANSHEL ET AL.) 19 November 1996, abstract	1-23
A	US 5,497,423 A (MIYAJI) 05 March 1996, abstract	1-23



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
A document defining the general state of the art which is not considered to be of particular relevance		
B earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
O document referring to an oral disclosure, use, exhibition or other means	"&"	document member of the same patent family
P document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
01 MARCH 1999

Date of mailing of the international search report

12 APR 1999

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer

DOUGLAS MEISLAHN

Telephone No. (703) 305-1338

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US98/25824

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A /	US 5,463,690 A (CRANDALL) 31 October 1995, abstract	1-23
A /	US 5,442,707 A (MIYAJI ET AL.) 15 August 1995, abstract	1-23
A /	US 5,373,560 A (SCHLAFLY) 13 December 1994, abstract	1-23
A /	US 5,159,632 A (CRANDALL) 27 October 1992, abstract	1-23

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US98/25824

B. FIELDS SEARCHED

Electronic data bases consulted (Name of data base and where practicable terms used):

APS

search terms: elliptic curve and 380/#/icls, elliptic curve (p) (efficien? or improv? or optimiz? or accelerat?), elliptic curve crypto?

PATENT COOPERATION TREATY

REC'D 12 OCT 1999

PCT

WIPO PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

18

Applicant's or agent's file reference WWE-67196	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/US98/25824	International filing date (day/month/year) 04 DECEMBER 1998	Priority date (day/month/year) 05 DECEMBER 1997
International Patent Classification (IPC) or national classification and IPC IPC(6): H04L 9/30 and US Cl.: 380/28, 30		
Applicant SECURED INFORMATION TECHNOLOGY, INC.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets.

This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority. (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 0 sheets.

3. This report contains indications relating to the following items:

- I Basis of the report
- II Priority
- III Non-establishment of report with regard to novelty, inventive step or industrial applicability
- IV Lack of unity of invention
- V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI Certain documents cited
- VII Certain defects in the international application
- VIII Certain observations on the international application

Date of submission of the demand 25 JUNE 1999	Date of completion of this report 06 AUGUST 1999
Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer TOD SWANN Telephone No. (703) 305-1338
Facsimile No. (703) 305-3230	<i>Joni Hill</i>

L Basis of the report

1. This report has been drawn on the basis of (Substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments):

the international application as originally filed.

the description, pages 1-46, as originally filed.

pages NONE, filed with the demand.

pages NONE, filed with the letter of _____.

pages _____, filed with the letter of _____.

the claims, Nos. 1-23, as originally filed.

Nos. NONE, as amended under Article 19.

Nos. NONE, filed with the demand.

Nos. NONE, filed with the letter of _____.

Nos. _____, filed with the letter of _____.

the drawings, sheets/fig NONE, as originally filed.

sheets/fig NONE, filed with the demand.

sheets/fig NONE, filed with the letter of _____.

sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

the description, pages NONE.

the claims, Nos. NONE.

the drawings, sheets/fig NONE.

3. This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the **Supplemental Box**. Additional observations below (Rule 70.2(c)).

4. Additional observations, if necessary:

NONE

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/US98/25824

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**1. STATEMENT**

Novelty (N)	Claims <u>1-23</u>	YES
	Claims <u>NONE</u>	NO
Inventive Step (IS)	Claims <u>1-23</u>	YES
	Claims <u>NONE</u>	NO
Industrial Applicability (IA)	Claims <u>1-23</u>	YES
	Claims <u>NONE</u>	NO

2. CITATIONS AND EXPLANATIONS

Claims 1-23 meet the criteria set out in PCT Article 33(2)-(4), because the prior art does not teach or fairly suggest mapping in elliptic curve cryptography as taught by the applicant.

----- NEW CITATIONS -----
NONE



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L 9/30		A1	(11) International Publication Number: WO 99/30458 (43) International Publication Date: 17 June 1999 (17.06.99)
(21) International Application Number: PCT/US98/25824 (22) International Filing Date: 4 December 1998 (04.12.98) (30) Priority Data: 60/069,314 5 December 1997 (05.12.97) US		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(71) Applicants (for all designated States except US): SECURED INFORMATION TECHNOLOGY, INC. [US/US]; Suite 315, 5700 Wilshire Boulevard, Los Angeles, CA 90036 (US). THE STATE OF OREGON, acting by and through THE STATE BOARD OF HIGHER EDUCATION on behalf of OREGON STATE UNIVERSITY [US/US]; Corvallis, OR 97331 (US).		Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>	
(72) Inventors; and (75) Inventors/Applicants (for US only): KOC, Cetin, Kaya [US/US]; 1250 Northwest 17th Street, Corvallis, OR 97330 (US). BEAHAN, John, Jr. [US/US]; Apartment 12, 170 Chester Avenue, Pasadena, CA 91106 (US). SADEGHI, Behzad [IR/US]; Apartment 12, 170 South Chester Avenue, Pasadena, CA 91106 (US).			
(74) Agent: HEEG, Suzanne, J.; Sheppard Mullin Richter & Hampton LLP, 48th floor, 333 South Hope Street, Los Angeles, CA 90071 (US).			

(54) Title: TRANSFORMATION METHODS FOR OPTIMIZING ELLIPTIC CURVE CRYPTOGRAPHIC COMPUTATIONS

(57) Abstract

The present invention provides a transformation method for obtaining optimized hardware and software implementations of elliptic curve cryptographic systems, including elliptic curve encryption, decryption, and signature functions. The method is applicable to any elliptic curve group G defined over any field F . More specifically, the present invention is characterized by speeding up the elliptic curve point multiplication operation, which consists of the calculation $Q = eP$, where P is a member of G and e is an integer. This is achieved by transforming $P = (x, y)$ to a point $P' = (x', y')$ in order to compute $Q' = (u, v = eP')$. The point P' is not necessarily on the elliptic curve, but by performing calculation on P' and transforming the resulting Q' back into G , it may be possible to calculate Q more efficiently than utilizing a direct method. The present invention also includes a method for optimizing the calculation of cryptographic operations involving arbitrary expressions in finite field arithmetic through a transformation method that permits the use of any field F in an efficient manner. The invention includes a method for optimizing arbitrary finite calculation in any finite field. The present invention teaches a set of transformations of cryptographic calculations that allows the use of other known techniques that have only been applicable to certain limited special cases prior to this invention.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/25824

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/30
US CL :380/28, 30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/28, 30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,E	US 5,854,759 A (KALISKI, JR. ET AL.) 29 December 1998, abstract	1-23
A,P	US 5,805,703 A (CRANDALL) 08 September 1998, abstract	1-23
A,P	US 5,751,808 A (ANSHEL ET AL.) 12 May 1998, abstract	1-23
A	US 5,581,616 A (CRANDALL) 03 December 1996, abstract	1-23
A	US 5,577,124 A (ANSHEL ET AL.) 19 November 1996, abstract	1-23
A	US 5,497,423 A (MIYAJI) 05 March 1996, abstract	1-23

 Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:	*T*	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
A document defining the general state of the art which is not considered to be of particular relevance	*X*	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
E earlier document published on or after the international filing date	*Y*	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*&*	document member of the same patent family
O document referring to an oral disclosure, use, exhibition or other means		
P document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search

01 MARCH 1999

Date of mailing of the international search report

12 APR 1999

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

DOUGLAS MEISLAHN

Telephone No. (703) 305-1338

Jane Hill

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/25824

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,463,690 A (CRANDALL) 31 October 1995, abstract	1-23
A	US 5,442,707 A (MIYAJI ET AL.) 15 August 1995, abstract	1-23
A	US 5,373,560 A (SCHLAFLY) 13 December 1994, abstract	1-23
A	US 5,159,632 A (CRANDALL) 27 October 1992, abstract	1-23

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US98/25824

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.: 1-23
because they relate to subject matter not required to be searched by this Authority, namely:

The claims are to a mathematical theory. However, in accordance with the office's policy, a search has been done according to US standards.
2. Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

The additional search fees were accompanied by the applicant's protest.

No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/25824

B. FIELDS SEARCHED

Electronic data bases consulted (Name of data base and where practicable terms used):

APS

search terms: elliptic curve and 380/###/icls, elliptic curve (p) (efficien? or improv? or optimiz? or accelerat?), elliptic curve crypto?